Applicants:	Liqun Chen, Keith A. Harrison, and David Soldera		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Method And Apparatus For Use In Relation To Verifying An Association Between Two Parties		
Serial No.:	10/613,522	Filing Date:	July 2, 2003
Examiner:	Shanto Abedin	Group Art Unit:	2436
Docket No.:	300202699-3		

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF PRIOR INVENTION PURSUANT TO 37 C.F.R. § 1.131

We, Liqun Chen, Keith A. Harrison, and David Soldera, hereby declare that:

1. We invented the subject matter claimed in US Pat. App. No. 10/613,522;

2. Our invention of the claimed subject matter in U.S. Pat. App. No. 10/613,522 was made before March 21, 2002, while we were working in Bristol, England for Hewlett-Packard Company;

3. The "Invention Proposal" dated February 22, 2002, a copy of which is attached to this declaration, was prepared before March 21, 2002;

4. The "Invention Proposal" shows conception and reduction to practice of the invention claimed in U.S. Pat. App. No. 10/613,522; and

5. We proceeded with due diligence beginning prior to March 21, 2002 to the filing of GB Pat. App. No. 0215590.1 in Great Britain on July 5, 2002, which led to the filing of the

PATENT LAW OFFICES OF
DAVID MILLERS
1221 Sun Ridge Road
Placerville, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

above-identified patent application in the United States of America on July 2, 2003, with a claim of priority to GB Pat. App. No. 0215590.1.

Each of us hereby declares that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Liqun Chen

Liqun Chen — Date: 19/2/2009

K A Harrison

Keith A. Harrison — Date: 19/2/2009

D Soldera

David Soldera — Date: 23/2/2009

(This document may be executed in counterpart.)

PATENT LAW OFFICES OF
DAVID MILLERS
1221 Sun Ridge Road
Placerville, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

[illegible] INVENTION PROPOSAL [illegible] PAGE(S) [illegible] OF [illegible]
[illegible] DATE RCVD [illegible] ATTORNEY [illegible]

Instructions: The information contained in this document is ***HP CONFIDENTIAL*** and may not be disclosed to others without prior authorization. Submit this document to the HP Intellectual Property Section as soon as possible. No patent protection is possible until a patent application is authorized, prepared, and submitted.

DESCRIPTIVE TITLE OF INVENTION:

An approach of hierarchical identifier-based cryptography using a key binding technique

FOR EACH INVENTOR PROVIDE THE FOLLOWING INFORMATION:
NB. If there are any non-HP employees involved, please make this clear & provide details (see below)

Employee No.	Full Name	Telnet	Entity & Lab Name	Home address:	Nationality
464932	Liqun Chen	3128217	TESL	1 Harvest Close Bradley Stoke Bristol, BS32 9DQ	British
	Keith Harrison				
	David Soldera				

Name all HP Division(s)/Lab(s) and related Project(s) to which the invention may be relevant (if known):

IBE project, TSP group, TESL, HPLB

Are there any plans to publish information describing the invention outside HP? If so, complete the following
- **i) date of publication:**
- **ii) article of publication:**

Are there any plans to use the invention in a HP product or prototype? If so, complete the following
- **i) product name:**
- **ii) date and location of first confidential release outside of HP of the product(s) or prototype:**
- **iii) date and location of first non-confidential release outside of HP of the product(s) or prototype:**

Is the invention likely to be standard related? If so, complete the following
- **i) related standard(name and version number):**

If any non-confidential disclosure have already occurred or will occur within 3 months, call your HP IP attorney NB. Public disclosure prior to filing a patent application at a Patent Office destroys the chance of patenting in most countries

CONTRACTUAL ASPECTS:

Was the invention made in the course of normal in-house HP R&D, without the involvement of any third party?

If not, please provide brief details:

DESCRIPTION OF INVENTION: *Please preserve all records of the invention and supply a brief description covering:*

A) SUMMARY OF THE INVENTION *(preferably one or two sentences that encapsulate the inventive concept; i.e. the difference between the invention and known prior art)*

This disclosure is attempted to propose a hierarchical identifier-based cryptography approach. The architecture of the hierarchy is based on zero knowledge proof of key binding. This approach can work with most of existing Identifier-Based Cryptography (IBC) schemes implemented by using either the Weil pairing or the Tate pairing to provide multiple levels of Trusted Authorities (TAs). By the term of IBC, we mean both Identifier-Based Encryption (IBE) and Identifier-Based Signature (IBS).

The major difference from known prior art is that this approach allows a TA in one level of the hierarchy (say TA_1), given a master private key generated by a TA in a higher level of the hierarchy (say TA_0), to generate his/her own private/public key pairs without further interaction with TA_0. There is no certificate needed in this hierarchy. The public key corresponding to the private key generated by TA_1 can be universally verified. Upon the verification successful, a verifier can be convinced that the one who must have knowledge of the TA1's master private key has created this private key; so either TA_1 or any other TAs in a higher level of the hierarchy is able to generate this key. The verification is a zero knowledge proof, which doesn't disclose the private key to the verifier.

This approach provides a different solution rather than existing certificate based hierarchical solutions in the manner of having better flexibility.

B) DOES THE INVENTION SOLVE A NEW OR EXISTING PROBLEM? IF SO, INDICATE THE PROBLEM AND ANY EXISTING SOLUTIONS, IF ANY, TO THIS PROBLEM AND DESCRIBE HOW THE PROBLEM IS SOLVED BY THE INVENTION

A number of IBC schemes from the Weil pairing and/or the Tate pairing have recently been published. All of these schemes involve a TA to provide services for an end user authorization and private key generation. For the purposes of making IBC technology more scalable, it is required to have a hierarchy of TAs, which provides the following feature: the root TA can issue private keys for other TAs in a lower level, who is turn can issue private keys for other TAs in a further lower level. All of these keys must be verifiable.

A straightforward method to solve the problem is using certificate with digital signatures. However, it requires interactions between certificate requestor and issuer.

This disclosure proposes a new hierarchical approach for IBC schemes, where there is one root TA in the top level and other TAs in different levels. The root TA has a master key, which is the master key of the whole hierarchy. Except for the root TA, each TA obtains her/his master private key from an above level TA. Based on this master private key, s/he can generate one or more pseudo-master private keys for her/himself. By using zero knowledge proof technology, the combination of the above level TA's master key, this TA's master key and this TA's pseudo-master key can be universally verified. So the architecture of the hierarchy can be verified without certification.

C) KNOWN PRIOR ART *(this should include details on any prior art searches that have been conducted including sources and key words used – a guide to searching can be found at* **http://lib.hpl.hp.com/bristol/prior_art_process.doc** *)*

The idea of hierarchical identifier-based cryptography has recently been addressed by Horwitz and Lynn. They proposed a hierarchical IBC and their paper is going to be published in Eurocrypt 2002. However, their scheme has a domain-collusion problem: more than *n* user colluded can discover a TA's master key. To solve this problem, they proposed a domain-collusion resistant scheme. To our understanding, this scheme has two major disadvantages: (1) it is very complicated; (2) it is not flexible – if the number of users in a domain increased to more than *n*, all of keys in the domain including the TA's master key and the users' keys must be regenerated.

So, their solution is not practical.

D) HOW TO IMPLEMENT THE INVENTION INCLUDING, WHERE APPROPRIATE, DRAWINGS (for guidance on the

amount and type of detail required see examples at http://legal.hp.com/patenttm/ag17/ag17pc.htm)

Here is an example of how to implement our hierarchy based on key binding for IBC. This example includes two TA levels. It is obvious that the implementation can be extended to more than two TA levels.

There are four entities involved in this implementation – a company (say HP) that is a root TA of the hierarchy, a laboratory (say TESL) that is a middle level TA of the hierarchy, an employee (say Bob) who is an end user of the hierarchy, and a business partner of HP (say Alice) who is a verifier of the hierarchy.

Let G_1 and G_2 denote two groups of prime order q in which the discrete logarithm problem is believed to be hard and for which there exists a computable bilinear map
$e: G_1 \times G_1 \rightarrow G_2$,
where e is a Weil/Tate pairing, G_1 is the group of points on an elliptic curve and G_2 is a subgroup of the multiplicative group of a finite field.

To setup the root TA - HP, HP should do the following:

1. Choose an arbitrary $P \in G_1$, optionally set P = MapToPoint (H (HP)) $\in G_1$.
2. Select a random $s \in \mathbb{Z}^*_q$ as HP's master private key.
3. Set a corresponding public key sP.

To setup the middle level TA - TESL, HP should do the following:

1. Compute MapToPoint (H (TESL)) = $Q \in G_1$.
2. Set TESL's master private key sQ.

To create TESL's pseudo-master private key, TESL should do the following:

1. Select a random $r \in \mathbb{Z}^*_q$ as TESL's pseudo-master private key.
2. Set the corresponding public parameters rsQ, rP and rQ.

Note that TESL can have more than one pseudo-master key from a single master private key sQ.

To register Bob, TESL should do the following:

1. Compute MapToPoint (H (Bob)) = $R \in G_1$.
2. Set Bob's private key rR.

Based on the following two checks:
$e(rP, Q)$?=? $e(P, rQ)$; and
$e(P, rsQ)$?=? $e(sP, rQ)$,
Alice can verify the "meaning" of rsQ, rP and rQ. In particular, she can convince herself that rsQ includes sQ and it must be generated by either HP or TESL, given that she has access to an authenticated copy of P and sP.

Then, to use those existing IBC algorithms (ref to our previous disclosure 300201957), we can replace (P, sP) with either (P, rP) or (Q, rQ), and as well as replace $e(R, sP) = e(sR, P)$ with $e(R, rP) = e(rR, P)$ or $e(R, rQ) = e(rR, Q)$.

Compared with the Horwitz and Lynn's hierarchical IBE scheme, there is no domain-collusion problem in our approach. So our approach is more efficient and flexible than their one.

THE INVENTION DISCLOSURE WAS SUBMITTED BY (i.e. the person responsible for completing the invention disclosure):					
Employee No.	Full Name	Telnet	Entity & Lab Name	Home address:	Nationality
464932	Liqun Chen	3128217	TESL	1 Harvest Close Bradley Stoke Bristol, BS32 9DQ	British
DATE: 22nd February 2002					

(If you do not know who your IP Attorney is, you can call Denise Kilgannon, TelNet 312-8228)